



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,047	08/23/2000	Alexandr Andreevich Moldovyan	P65855US0	4150

136 7590 05/14/2004

JACOBSON HOLMAN PLLC  
400 SEVENTH STREET N.W.  
SUITE 600  
WASHINGTON, DC 20004

EXAMINER
----------

CURCIO, JAMES A F

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/14/2004

3

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/622,047

Applicant(s)

MOLDOVYAN ET AL.

Examiner

James Curcio

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 23 August 2000.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-4 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4 is/are rejected.
- 7) ☒ Claim(s) 1 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

***Claim Objections***

1. Claim 1 objected to because of the following informalities: "on on" should be "on" in line 5. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-4 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The following phrases in claim 1---"alternate converting said subblocks" and "dual-locus operation"---are vague, indefinite, and lack a corresponding definition in the specification.

Also, in claim 1, the clause "a conversion operation is performed on the subkey depending on j-th subblock" is ambiguous and thus, is vague and indefinite. It is unclear from this phrase whether the value, form, and/or choice of the subkey depends on the j-th subblock, whether the choice of which conversion operation to be performed depends on the j-th subblock, or whether the choice of executing or not executing the conversion operation depends on the j-th subblock. It is also unclear from the phrase whether "the subkey" refers to the i-th subkey, the j-th subkey, or any subkey.

The phrases "operation of permuting subkey bits depending on said j-th subblock", "operation of cyclic offsetting subkey bits depending on said j-th subblock",

Art Unit: 2132

and "substitution operation performed on a subkey depending on said j-th subblock" in respective claims 2, 3, and 4 have a similar structural ambiguity. It is unclear whether the operations in these phrases depend on the "said j-th subblock" or whether the subkey or subkey bits depend on the j-th subblock. It is also unclear from the phrases whether "subkey" refers to the i-th subkey, the j-th subkey, or any subkey.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claim 1 rejected under 35 U.S.C. 102(e) as being anticipated by Den Boer (US006298136B1). Den Boer discloses the following method steps:

- a. generating an encryption key (claim 9; column 4, lines 35-65; and column 5, lines 26-57)

Art Unit: 2132

- b. breaking down a data block (claim 9; column 4, lines 35-65; and column 5, lines 26-57)
- c. alternate converting said subblocks by performing a dual-locus operation (claim 9; column 4, lines 35-65; and column 5, lines 26-57)
- d. performing a conversion operation on the subkey depending on the j-th subblock (claim 9; column 4, lines 35-65; and column 5, lines 26-57)

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 2-4 rejected under 35 U.S.C. 103(a) as being unpatentable over Den Boer (US006298136B1) as applied to claim 1 above, and further in view of Coppersmith et al (US006192129B1).

8. As per claims 2 and 4, as described in the teachings applied above with respect to claim 1, Den Boer discloses a method for block encryption of discrete data comprising steps a-d. Den Boer does not expressly disclose either an operation of . permuting subkey bits or a substitution operation performed on a subkey as being the conversion operation of step d. However, Coppersmith et al discloses such operations as prior art (Coppersmith et al – column 22, lines 1-5 and 44-45 and column 23, lines 15-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Den Boer to include either the

Art Unit: 2132

operation of permuting subkey bits or the substitution operation performed on a subkey as the j-th subblock-dependent conversion operation as per the teachings disclosed in Coppersmith et al. One of ordinary skill in the art would have been motivated to do so in order to generate multiple distinct keys for the multiple rounds of the encryption algorithm (Coppersmith et al – column 2, lines 11-13).

9. As per claim 3, as described in the teachings applied above with respect to claim 1, Den Boer discloses a method for block encryption of discrete data comprising steps a-d. Den Boer does not expressly disclose an operation of cyclic offsetting subkey bits as being the conversion operation of step d. However, Den Boer discloses such an operation as prior art (column 2, lines 1-15). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Den Boer to include the operation of cyclic offsetting subkey bits as the j-th subblock-dependent conversion operation as per the disclosed prior art. One of ordinary skill in the art would have been motivated to do so in order to generate multiple distinct keys for the multiple rounds of the encryption algorithm (Coppersmith et al – column 2, lines 11-13).

### ***Conclusion***

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Curcio whose telephone number is 703-305-8887. The examiner can normally be reached on Tuesday through Friday from 7 am to 5 pm.

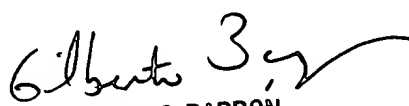
Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on Monday through Friday. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

je

April 29, 2004  
JC  
AU2132

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100